INTERNET 2

2017 TECHNOLOGY exchange

SAN FRANCISCO CA   OCTOBER 15–18

CINC UP: CYBERSECURITY RESEARCH ACCELERATION WORKSHOP AND SHOWCASE

Brought to you by CENIC and Internet2

JOHN DUNDAS

VP and CTO, CENIC

FLORENCE HUDSON

SVP & Chief Innovation Officer, Internet2

CINC UP: CYBERSECURITY RESEARCH ACCELERATION WORKSHOP & SHOWCASE
AGENDA

- Welcome and Introduction
- CIO & Industry Perspective
- NSF Program Director Update
- Cybersecurity Research Panel: Network Security
- Cybersecurity Research Panel: Internet of Things
- Cybersecurity Research Panel: Identity & Access Management
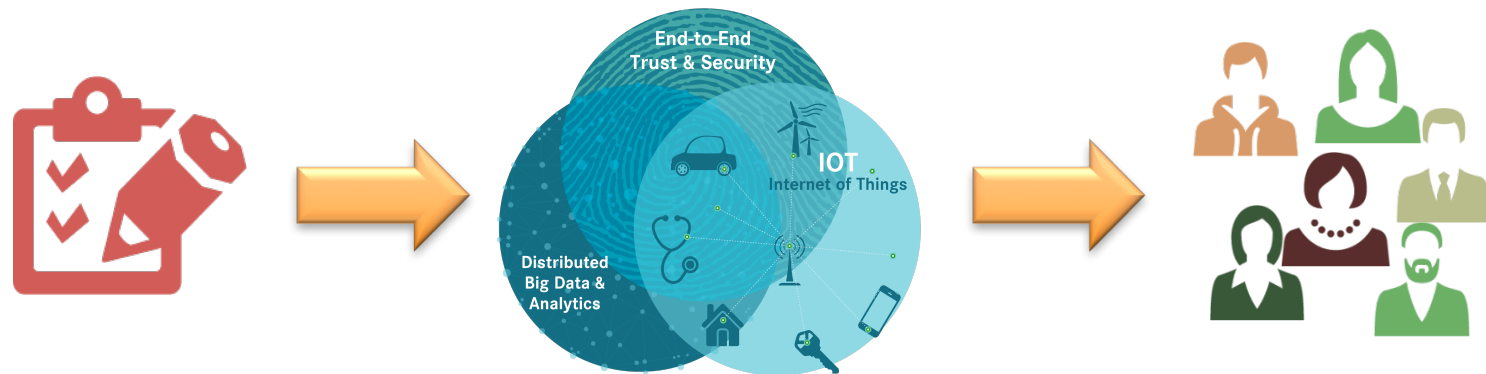- Cybersecurity Research Panel: Multidisciplinary Cybersecurity

Welcome and Introduction

Internet2 Collaborative Innovation Community was created in 2015 based on a member survey of 8,800 individuals identifying their top areas of interest for open, inclusive, collaborative innovation.

- Three Innovation Working Groups launched at Global Summit in May 2015
- Now, 400+ Collaborative Innovation Community (CINC UP) participants, representing 170+ institutions (as of October 2017)

Internet2 CINC UP combines three member-led innovation working groups, focused on areas brought forward by members, related to our top two priorities of advanced networking plus trust & identity.

E2E Trust & Security (E2ET&S)
- **TIPPSS for IoT – Trust, Identity, Privacy, Protection, Safety, Security**
- **NSF EAGER Cybersecurity Transition to Practice Acceleration**
- **SDP (Software Defined Perimeter), Network Segmentation for IoT**

Distributed Big Data & Analytics (DBDA)
- **NSF Big Data Hub Collaboration**
- **Smart Campuses and Cities**
- **Health & Life Sciences / Genomics**
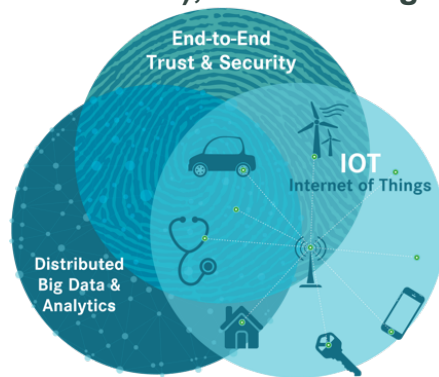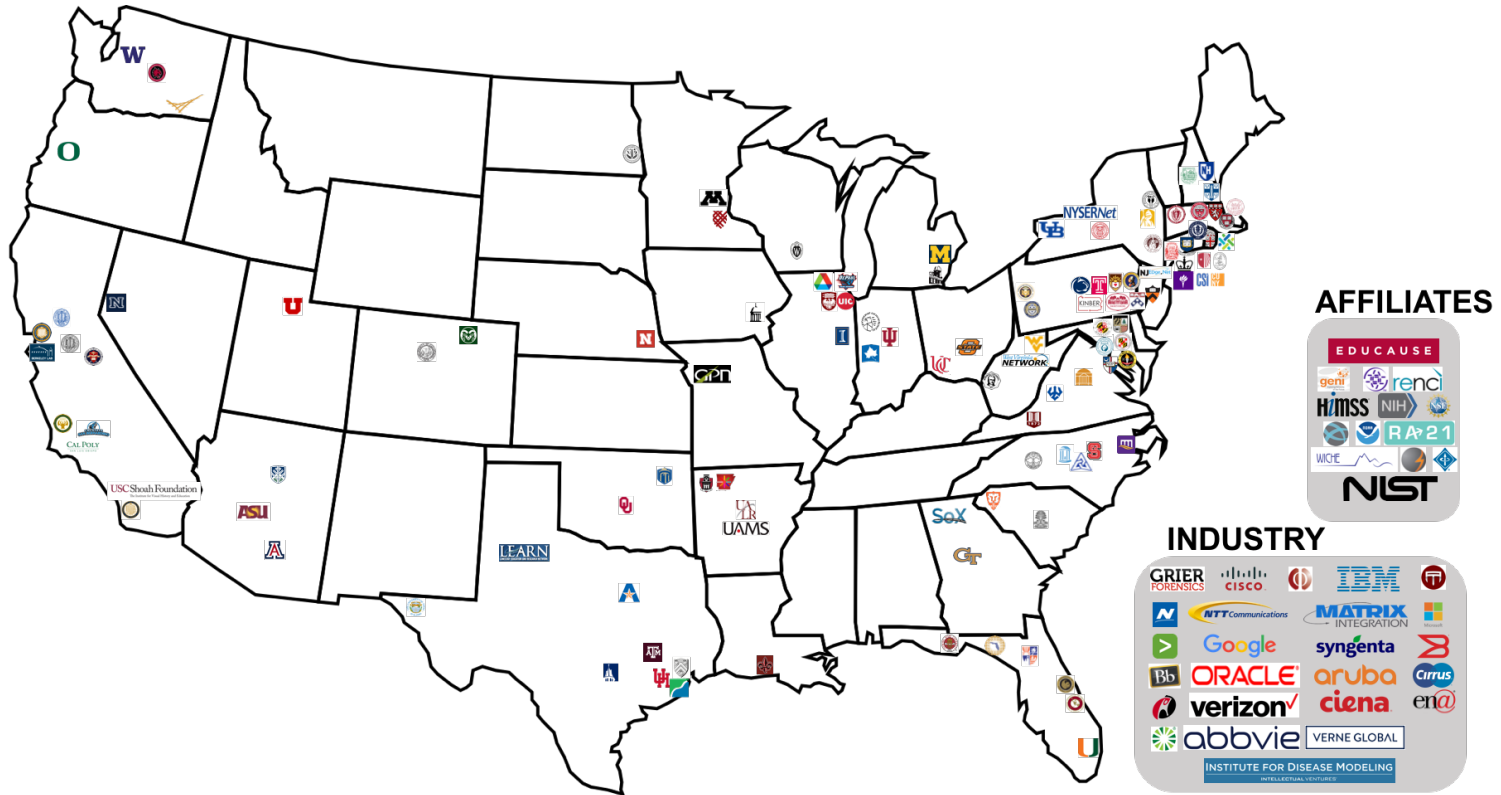
Internet of Things (IoT)
- **IoT Sandbox**
- **Smart Campuses and Cities**
- **Smart Grid Testbed**

Join us! Email CINO@Internet2.edu

Internet2 CINC UP in the US has grown to 380+ individuals, from 155+ organizations, representing 31% of Internet2 member institutions.

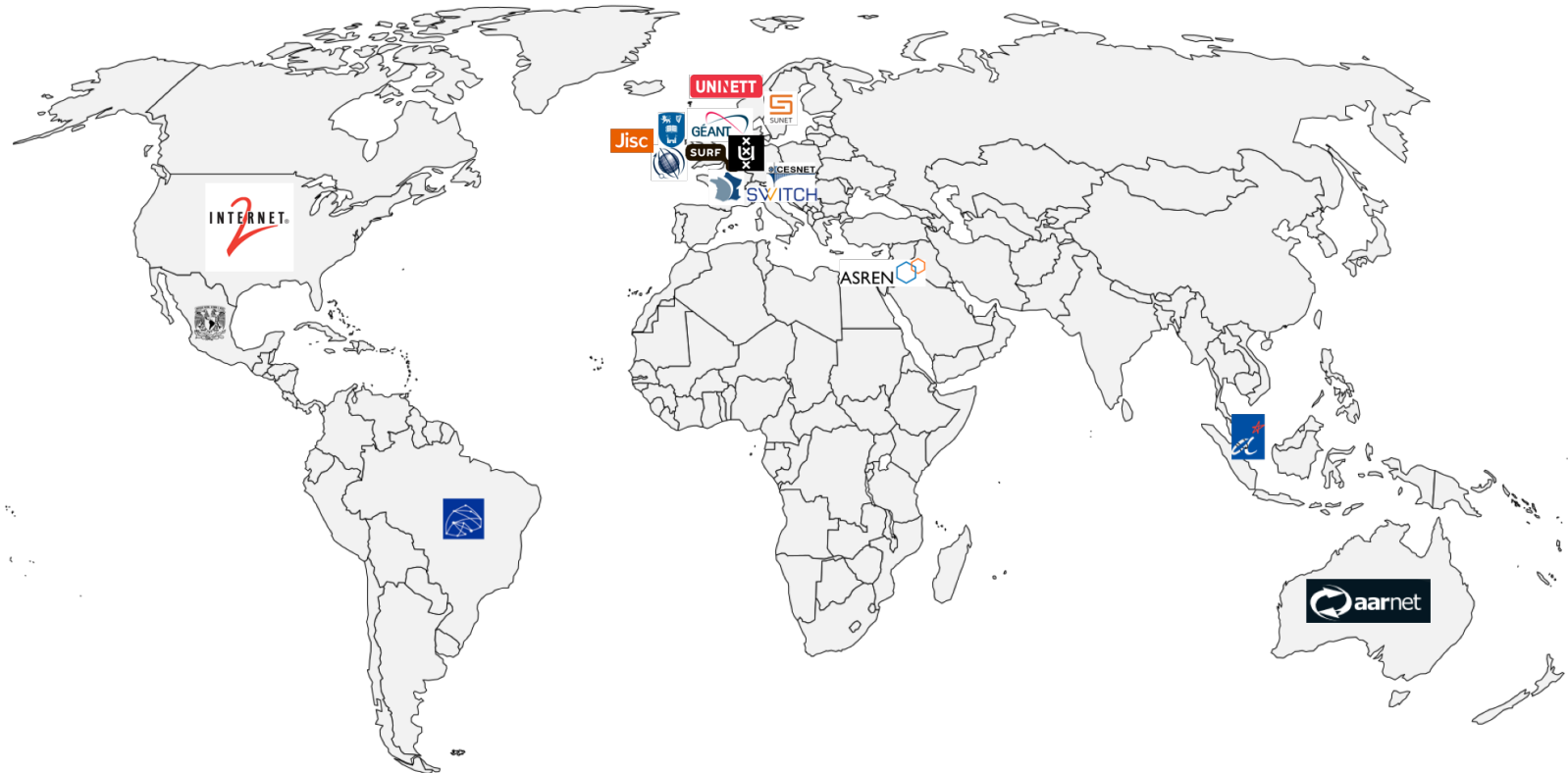**Globally, the Internet2 Collaborative Innovation Community has grown to 400+ individuals, from 170+ organizations.**

As of October 6, 2017

INTERNET2 | 2017 TECHNOLOGY exchange | OCTOBER 15-18 | SAN FRANCISCO CA

NSF EArly-concept Grant for Exploratory Research (EAGER): Cybersecurity Transition To Practice (TTP) Acceleration

Challenge

- **Accelerate Transition To Practice (TTP)** of NSF-funded later-stage cybersecurity research into **Research & Education environments**

Solution

- Identify & assess NSF cybersecurity research **inventory**

- **Interview** researchers & practitioners for cybersecurity TTP needs, gaps and best practices

- **Leverage Internet2 community** to enable "matchmaking"

- Deploy webinars, portal, in-person **events for researcher/IT matchmaking**

    – San Francisco, Oct 18,12:30-5:30pm

Cybersecurity Research Assets:
- NDN
- CILogon 2.0
- CipherLocker
- …
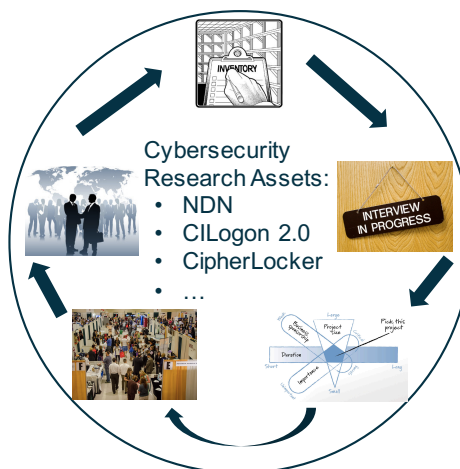
Award Number: 1650445
Internet2
August 2016 – August 2018
PI: Florence Hudson, SVP/Chief Innovation Officer
Team: Emily Nichols, Giselle Trent, Bruce Maas

Scientific Impact

- **Increase awareness** of cybersecurity research & capabilities

- **Accelerate cybersecurity TTP** to make cyberspace safer

- **Identify cybersecurity needs** to inform future research

Broader Impact

- Enable **partnership for NSF TTP with other Federal agency programs** to accelerate & streamline TTP pipeline

- **Enable more diverse R&E pipeline** partnering with Society of Women Engineers and others

- We need you in cybersecurity

SME Interview insights regarding TTP acceleration informed the EAGER project plan

Cybersecurity Researchers

- Key needs for TTP identified: Funding from NSF and others, **early user feedback**
- **User feedback from pilot deployments** critical to accelerate TTP
- Opportunity for acceleration of the TTP process at multiple steps
- Researchers like opportunity to leverage NSF TTP, DHS TTP, I-CORPS **multiple agency support**
- TTP not a priority for some researchers – looking to solve complex problems, not start a business

Practitioners for Pilot Deployments

- Practitioners **need to know operational requirements** for pilot use of TTP assets
- All size universities and regional networks interested in potential to test out / pilot cyber research early
- Smaller universities requested to participate in TTP as they have simpler approval processes
- Some universities unwilling to deploy unproven, non-production tested cybersecurity code

Agencies

- Interested in **cross-agency collaboration** opportunities, e.g., for NSF and DHS, to accelerate cyber TTP

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

Researcher Assets:
http://bit.ly/ttptechexresearch

NSF Program Director Update

CIO & Industry Perspective

INTERNET2 · 2017 TECHNOLOGY exchange · OCTOBER 15–18 · SAN FRANCISCO CA

Panelists

Moderator: Bruce Maas, Innovation Fellow, Internet2

Larry Conrad, Associate Vice Chancellor for Information Technology and Chief Information Officer, University of California-Berkeley

Meredith Lee, Executive Director, West Big Data Innovation Hub, University of California-Berkeley

Michael Shepherd, Business Development Manager, Cisco Systems

Ruth Marinshaw, Chief Technology Officer – Research Computing, Stanford University

Bruce Taggart, Vice Provost for Library & Technology Services, Lehigh University

Panel Questions

- **Ruth Marishaw**, you bring the perspective of someone who is already working with faculty researchers in a significant way. And Stanford is already well known for working closely with the private sector. Where do you see opportunities at Stanford related to the TTP goals, and do you have a perspective to share on what kind of approach has worked there in the past?

- **Larry Conrad**, your job is to make sure that every service delivered by Berkeley IT works well all the time. In addition to that primary mission, you are also expected to respond to the needs and interests of a wide diversity of faculty and researchers. How do you envision how your organization could partner with faculty interested in TTP? Can you do this and still fulfill the mission or reliable, dependable services?

- **Meredith Lee,** What are you seeing in the Big Data Hub projects regarding cybersecurity challenges and opportunities? Where do you see some opportunities for researchers to utilize your own campus to advance their research?

- **Bruce Taggart**, you bring the unique experience of someone who is responsible for both library and IT at a research university. Plus, you are already engaged with researchers on your campus. Please discuss how you are collaborating on developing your "Campus as a Living Lab" concept (OSiSoft Data monitoring projects (energy), Cyber data (Scans, Attacks, Advanced Persistent Threats, et al). What has happened at Lehigh to enable this?

- **Mike Shepherd**, I view you as one of or the main points of contact with Internet2 and higher education. Can you elaborate on some of the opportunities Cisco sees coming from the TTP program? How can faculty conducting research that is of potential interest to Cisco navigate with you?

INTERNET® 2017 TECHNOLOGY exchange   OCTOBER 15–18   SAN FRANCISCO CA

Panel Questions

- Cybersecurity stakes continue to ratchet up. Recall that the CISOs and CIOs at both EquiFax and at Target were immediate casualties of their very public compromises followed shortly by the CEOs. How do we defend use of promising, but unproven information security technologies in the name of supporting research? What if a particular promising solution doesn't pan out?

- Higher education is steadily moving forward with closer collaboration with the private sector in both research, and workforce development. We have representatives of industry and higher education on this panel. What is the ideal relationship for you, and let's start with our industry panelist Mike.

Sample MOU

- UW Madison Cybersecurity Operations Center, Memorandum of Understanding for Faculty Research

- The University of Wisconsin Madison CIO Office *encourages collaboration between technology researchers and operations staff*. UW-Madison has one of the most complex learning and research laboratories in the form of its campus network and WAN. We *encourage researchers to share their research* with us in the hope that we can *help them to test out, deploy, and fine tune their intellectual property*. We view this as a win-win scenario.

- In order to ensure the highest level of communication between parties who do have different needs and experiences, it *is important to write down some of the basic understandings that each party has*. We refer to this as a Memorandum of Understanding. We are in the *process of developing a boilerplate MOU* to address some of the most important aspects, and are sharing this with other institutions to create a document which can be of value to other institutions as well.

Sample MOU

1. As part of the Office of Cybersecurity, the Cybersecurity Operations Center (CSOC) has been established to protect the University from cyber-attacks of all forms. As such, it is first and foremost an operations center with a primary mission to protect the university.

2. University *researchers need environments in which to experiment and innovate*. To the extent that their research can be conducted on the university network *without compromising operations*, it will be considered.

3. The *workload and mission needs of the CSOC will take priority* over the timeline and project needs of the researcher. However, every effort will be made to *balance expectations so that both needs can be addressed*. We understand that faculty research normally has a timeline, and at times intermediate deadlines, that can create a sense of urgency. *Discussing key deadlines and expectations up front will minimize disappointment and cross communication*.

4. For research projects that require *risk assessment and certifications* (e.g., systems under Federal research programs), *early contact with the Office of Cybersecurity is required* to ensure required documentation and testing is complete prior to the project beginning work.

5. If an *NDA* is required, this will be *discussed up front before any research begins*.

6. Staff and student staff will function effectively as extended members of the researcher's team. For that reason, it will be *important for the researcher and the CISO to build a sense of community* together. *This is a partnership*.

7. Within calendar year 2018 the CSOC and Office of Cybersecurity will begin to host a vendor provided service which may be used by researchers in the field of firewalls, intrusion detection and intrusion prevention for research projects.

Cybersecurity Research Panel: Network Security

INTERNET2 2017 TECHNOLOGY exchange   OCTOBER 15–18   SAN FRANCISCO CA

CINC UP: CYBERSECURITY RESEARCH ACCELERATION WORKSHOP & SHOWCASE

AGENDA

- **Cybersecurity Research Panel: Network Security**
  - Alberto Dainotti, University of California-San Diego
  - Dijiang Huang, Arizona State University
  - Johanna Amann, University of California-Berkeley
  - Clifford Neuman, University of California-Berkeley
  - Christos Papadopoulos, Colorado State University
  - Jun Li, University of Oregon
  - Jelena Mirkovic, University of Southern California
- **Cybersecurity Research Panel: Internet of Things**
  - Blaine Reeder, University of Colorado at Denver
- **Cybersecurity Research Panel: Identity & Access Management**
  - Kent Seamons, Brigham & Young University
  - Stanislaw Jarecki, University of California-Irvine
- **Cybersecurity Research Panel: Multidisciplinary Cybersecurity**
  - Shamik Sengupta, University of Nevada

Closing

Florence Hudson
SVP and Chief Innovation Officer, Internet2

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

Researcher Assets:
http://bit.ly/ttptechexresearch

INTERNET2

2017 TECHNOLOGY exchangə

SAN FRANCISCO CA   OCTOBER 15–18

CINC UP: CYBERSECURITY RESEARCH ACCELERATION WORKSHOP AND SHOWCASE

Brought to you by CENIC and Internet2

JOHN DUNDAS

VP and CTO, CENIC

FLORENCE HUDSON

SVP & Chief Innovation Officer, Internet2